IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.:	10/086,302
Inventor:	Alexander Medvinsky
Filing Date:	February 28, 2002
Title:	Detection of Duplicate Client Identities in a Communication System
Examiner:	Gelagay, Shewaye
Art Unit:	2137
Atty. Docket No.:	D02643

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Please enter this as an Appeal to the Examiner's Final Rejection mailed from the U.S. Patent and Trademark Office on May 7, 2007. The Notice of Appeal was filed on November 7, 2007.

(I) Real Party in Interest

General Instrument Corporation, a wholly owned subsidiary of Motorola, Inc., is the real party in interest.

(II) Related Appeals and Interferences

There are no related appeals or interferences known to the Applicant.

(III) Status of Claims

Claims 1-6, 8-12, 18, 20-22, and 24-26 are pending and presently stand twice and finally rejected and constitute the subject matter of this appeal.

Claims 1-6, 8, 11-12, 18, 20-22, and 24-26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,069,877 to Yang (hereinafter "Yang") in view of U.S. Publication Number 2002/0150253 to Brezak et al. (hereinafter "Brezak").

Claims 9-10 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Yang in view of Brezak and further in view of Tung et al., Public Key Cryptography for Initial Authentication in Kerberos (hereinafter "Tung").

Applicant appeals all pending claims 1-6, 8-12, 18, 20-22, and 24-26.

(IV) Status of Amendments

Applicant did not submit any After Final amendments in response to the Final Rejection mailed from the U.S. Patent and Trademark Office on May 7, 2007.

Applicant's most recent amendment to the claims was submitted on January 31, 2007, in response to the non-final Office Action dated September 28, 2006, and was entered by the Examiner. The claims as thus amended are included in Appendix A attached hereto.

(V) Summary of Claimed Subject Matter

Embodiments of the present invention concern a method, such as that recited by claim 1, for detecting clones (unauthorized duplicate identities) of a client. A first signal is forwarded from the client to a key distribution center (KDC), the first signal for requesting access to a server. *See* paragraph [36]. Following verification that the client is authorized to access the server, *see* paragraph [37], an authentication token including an encrypted session key is transmitted from the KDC to the client. *See* paragraph [40]. The authentication token is for providing access to the server, and is valid for a time T. *Id.* A second signal for requesting access to the server is received from an entity having identifying information identical to the client, prior to expiration of the time T, *see* paragraphs [43-46], and the entity is marked as a possible clone, or the second request is denied, in order to prevent access to the server. *See* paragraph [20], FIG. 2.

Other embodiments of the present invention concern a system, such as that recited by claim 4, for detecting clones of a client within a communication network, in which the system includes a KDC, an application server communicably coupled to the KDC, and a client for providing a first request to access the application server. *See* FIG. 1, paragraph [25]. In the system, responsive to the first request, the KDC forwards a first authentication token including an encrypted session key for accessing the application

server. *See* paragraph [36]. The first authentication token is valid for a time duration T. *See* paragraph [40]. The KDC receives a second request during time T to access the application server, the second request being received from an entity having identifying information identical to the client, *see* paragraphs [43-46], and the KDC denies the second request to prevent the entity from accessing the application server. *See* FIG. 2 and paragraphs [14] and [47-49].

Further embodiments of the present invention concern a system, such as that recited by claim 18, for detecting clones of a client within a communication network, in which the system includes a KDC, a server communicably coupled to the KDC, and a client for receiving an authentication token including an encrypted session key from the KDC. *See* FIG. 1, paragraph [25]. The authentication token is for accessing the server, and is valid for a time duration T. *See* paragraph [40]. In the system, the server receives from the client a first request to access the server, the first request being accompanied by the authentication token. The server records the time duration T for which the authentication token is valid. *See* paragraph [51]. The server receives from an entity having identifying information identical to the client, a second request during the time duration T to access the server, *see* paragraphs [43-46], and the server either flags or denies the second request to prevent access to the server. *See* FIG. 2 and paragraphs [20], [47-49], and [51].

Still further embodiments of the invention concern a method, such as that recited by claim 22, for detecting clones in a communication network. An authentication token for accessing a KDC, including an encrypted session key valid for a time duration T, is provided to an authorized client. A request is received during time T to access the KDC,

the request being received from an entity with the same identifying information as the authorized client. If the request is received during time T, the entity is flagged as a possible clone or the request to access to the KDC is denied. *See* FIG. 2 and paragraphs [14] and [47-49].

In each embodiment, if the access request is *prior to* expiration of the ticket previously issued to the authorized client, the access request is identified as a possible fraudulent request. *See* paragraph [14]. It is probable the access request is from a clone, because an authorized client would not keep requesting for tickets while its ticket is valid. *Id.* Such continuous requests, however, may occur when the authorized client loses it ticket, and for such cases, the access request is flagged for further investigation. *Id.*

(VI) Grounds of Rejection to be Reviewed on Appeal

Whether the rejection of claims 1-6, 8, 11-12, 18, 20-22, and 24-26 under 35 U.S.C. § 103(a) as being unpatentable over Yang in view of Brezak is proper.

Whether the rejection of claims 9-10 under 35 U.S.C. § 103(a) as being unpatentable over Yang in view of Brezak and further in view of Tung is proper.

(VII) Argument

Rejections under 35 U.S.C. §101

None.

Rejections under 35 U.S.C. §112, first paragraph

None.

Rejections under 35 U.S.C. §112, second paragraph

None.

Rejections under 35 U.S.C. §102

None.

Rejections under 35 U.S.C. §103

Group 1 – Claims 1-6, 8, 11-12, 18, 20-22, and 24-26

The rejections of claims 1-6, 8, 11-12, 18, 20-22, and 24-26 under 35 U.S.C. § 103(a) are respectfully traversed.

Independent claim 1 requires "receiving a second signal from an entity *prior to the expiration of the time T.*" Similarly, independent claim 4 requires "receiving a second request *during time T.*" Independent claim 18 requires "receiving from an entity, a second request *during the time duration T*" and claim 22 requires "receiving a request *during time T.*" Accordingly, in all of the independent claims of the present application, it is a required feature that "the second request" be received "prior to expiration of time T," "during time T" and "during a time duration T."

In the Final Office Action dated May 7, 2007, the Examiner states "[a]s per claim 1: Yang discloses a method for detecting clones (unauthorized duplicate identities) of the client, the method comprising: forwarding a first signal from a client, the first signal for requesting access to a server… verifying that the client is authorized to access the server… receiving a second signal from an entity prior to expiration of the time T, the second signal for requesting access to the server, wherein the entity has identifying information identical to the client… and marking the entity as a possible clone or denying the request in order to prevent access to the server...." Final Office Action, page 2-3.

Applicant respectfully disagrees that Yang discloses "receiving a second signal from an entity prior to expiration of the time T." The portions of Yang cited by the Examiner for this feature (col. 3, lines 59-67, and col. 4, lines 6-9) nowhere disclose the claimed limitation "prior to expiration of the time T."

To the contrary, Yang discloses no time restriction on receiving a second signal; the second signal may be received during an unbounded period, having no expiration. Upon receipt of the second signal, Yang teaches determining "if a session is already established in the system 50 . . . under the same apparent device ID as the mobile communication unit 66 currently already making the session request . . ." (col. 10, lines 66-67, and col. 11, lines 1-3). The determination taught by Yang occurs at any time upon receipt of the second signal, with no reference to any time period associated with the validity or expiration of an authentication token.

Accordingly, the Final Office Action is incorrect in its interpretation of Yang. Yang discloses a network cellular communication system where a mobile communication unit in the network attempts to register to the network and the network determines whether the mobile communication unit is already registered to the network by comparing identification codes. Specifically, if the identification code of the mobile attempting to register is a duplicate to an identification code of a mobile communication unit already registered to the network, the network refuses registration of the mobile communication unit attempting to register. Yang, col. 3, lines 1-6.

Applicant's claims require that a request for access be "received prior to … *expiration of [a] time T*" and "marking the entity as a possible clone or denying the … request in order to prevent access to the server." As demonstrated above, Yang

specifically makes no restriction as to when the attempt to register is received by the network. Thus, Yang does not disclose Applicant's claim to receiving a request "prior to … expiration of the time T." Because Yang does not disclose a claimed limitation, the Final Office Action incorrectly rejects Applicant's claims requiring such a limitation.

Not only does the network of Yang fail to take into account the *time* of the mobile communication unit's attempt to register, Yang *teaches away* from taking into account any time period associated with the validity or expiration of an authentication token. Yang teaches that an initial request table is maintained indefinitely (i.e., without expiration) until an end session request is expressly made: "The mobile communication unit 66 entered into the table will then ***only*** be cleared from the table 340 when the host computer receives an end session request from the same mobile communication unit 66." (Col. 11, lines 18-21, emphasis added.) Yang specifically teaches the advantages of such a system, citing "a strong need in the art for a system that detects and rejects a mobile communication unit which is attempting to register to a communication system . . . with a duplicate ID so that a mobile communication unit ***already registered*** to the communication system is not ***deregistered or dumped*** . . ." (Col. 2, lines 34-40.)

Even if Yang were combined with Brezak, or other prior art references, Applicant respectfully submits that Yang fails to provide a basis for a rejection under 35 U.S.C. § 103, at least because Yang expressly *teaches away* from receiving the second signal or request "prior to expiration of time T," "during time T" and "during a time duration T." Because Yang is an improper basis for rejecting Applicant's claims, the combination of Yang with Brezak, or other prior art references, also is an improper basis for rejecting Applicant's claims.

Brezak also fails to disclose the limitation, present in all of the independent claims of the present application, of marking the entity as a possible clone, or denying the request, in order to prevent access to the server *when the second request is received prior to the expiration of the time T*. In the present invention, it is the receipt of such a second request prior to the expiration of time T that indicates that the entity is a possible clone. The claimed embodiments of the present invention accordingly mark the entity as a possible clone, or deny the request, in order to prevent access to the server.

Conversely, in paragraph [0062] of Brezak, it is explained that "[t]o prevent resending authenticators, KDC 306 will reject any authenticator whose timestamp is *too old*" (emphasis added). That is, Brezak teaches rejecting a second request that is received *after* the expiration of a time T, while the present invention is concerned with a second request that is received *prior to* the expiration of a time T.

Brezak teaches that if, inter alia, the second request is *not* too old (i.e., "[i]f everything [discussed in the preceding paragraph] checks out"), the KDC will not reject the second request, and "will believe that this user is who they claim to be" (paragraph [0063]). It would be contrary to this teaching of Brezak to prevent access to the server by marking the entity sending such a signal as a possible clone or denying the request, as required by all of the independent claims of the present invention. Accordingly, Brezak expressly *teaches away* from rejecting a second signal or request that is received "prior to expiration of time T," "during time T" and "during a time duration T."

Even if Brezak were combined with Yang, or other prior art references, Applicant respectfully submits that Brezak fails to provide a basis for a rejection under 35 U.S.C. § 103, at least because Brezak expressly *teaches away* from rejecting a second signal or

request that is received "prior to expiration of time T," "during time T" and "during a time duration T." Because Brezak is an improper basis for rejecting Applicant's claims, the combination of Brezak with Yang, or other prior art references, also is an improper basis for rejecting Applicant's claims.

Since Brezak fails to supply features missing from Yang, the combination of Yang and Brezak cannot suggest the invention and cannot render the claims obvious. Thus, no matter how Yang and Brezak may be combined (even assuming, arguendo, that one of ordinary skill in the art would be led to combine them) the resulting combination is not the invention recited in any of independent claims 1, 4, 18 and 22. Likewise, dependent claims 2, 3, 24, and 25 which depend on claim 1 and incorporate all of the limitations thereof are similarly patentable. Dependent claims 5, 6, and 8-12 which depend on claim 4 and incorporate all of the limitations thereof are similarly patentable. Dependent claims 20, 21, and 26 which depend on claim 18 and incorporate all of the limitations thereof are similarly patentable.

Accordingly, Applicants respectfully request withdrawal of the rejection of claims 1-6, 8, 11-12, 18, 20-22, and 24-26 under 35 U.S.C. § 103(a).

Group 2 – Claims 9-10

The rejections of claims 9-10 under 35 U.S.C. § 103(a) are respectfully traversed. Claims 9-10 are allowable at least because claims 9-10 depend from independent base claim 4, which is an allowable base claim for at least the reasons discussed with respect to Group 1 above.

Furthermore, even if Yang and Brezak were combined with Tung, or other prior art references, Applicant respectfully submits that Yang and Brezak both fail to provide a basis for a rejection under 35 U.S.C. § 103, at least because Yang and Brezak expressly *teach away* from receiving the second signal or request "prior to expiration of time T," "during time T" and "during a time duration T." Because Yang and Brezak are each an improper basis for rejecting Applicant's claims, the combination of Yang and/or Brezak with Tung, or other prior art references, also is an improper basis for rejecting Applicant's claims.

Accordingly, Applicants respectfully request withdrawal of the rejection of claims 9 and 10 under 35 U.S.C. § 103(a).

(VIII) Claims Appendix

A copy of the currently pending claims is attached.

(IX) Evidence Appendix

No additional evidence is provided in an evidence appendix.

(X) Related Proceedings Appendix

No related proceedings are provided in a related proceedings appendix.

Respectfully submitted,

ALEXANDER MEDVINSKY

Date: January 7, 2008

BY: /Stewart M. Wiener/
Stewart M. Wiener
Registration No. 46,201
Attorney for Applicant

MOTOROLA, INC.
101 Tournament Drive
Horsham, PA 19044
Telephone: (215) 323-1811
Fax: (215) 323-1300

CLAIMS APPENDIX

1. (Previously presented) A method for detecting clones (unauthorized duplicate identities) of the client, the method comprising:

forwarding a first signal from a client to a KDC, the first signal for requesting access to a server;

verifying that the client is authorized to access the server;

transmitting an authentication token including an encrypted session key from the KDC to the client, the authentication token for providing access to the server, wherein the authentication token is valid for a time T;

receiving a second signal from an entity prior to expiration of the time T, the second signal for requesting access to the server; wherein the entity has identifying information identical to the client; and

marking the entity as a possible clone or denying the second request in order to prevent access to the server.

2. (Previously presented) The method of claim 1 wherein the encrypted session key is valid for a designated duration.

3. (Previously presented) The method of claim 2 wherein the designated duration is for determining the time T for which the authentication token is valid.

4. (Previously presented) A system for detecting clones of a client within a communication network, the system comprising:

a KDC;

an application server communicably coupled to the KDC;

a client for providing a first request to access the application server;

responsive to the first request, the KDC forwarding a first authentication token including an encrypted session key for accessing the application server; the first authentication token being valid for a time duration T;

the KDC receiving a second request during time T to access the application server, the second request being received from an entity having identifying information identical to the client; and

the KDC denying the second request to prevent the entity from accessing the application server.

5. (Original) The system of claim 4 wherein the entity is a clone.

6. (Original) The system of claim 5 wherein the identifying information is a client identifier copied by the clone.

7. (Cancelled)

8. (Previously presented) The system of claim 4 further comprising the client deriving a copy of the encrypted session key for accessing the application server.

9. (Previously presented) The system of claim 8 wherein the encrypted session key is derived using a key agreement algorithm.

10. (Original) The system of claim 9 wherein the key agreement algorithm is the Diffie-Hellman algorithm.

11. (Original) The method of claim 1 further comprising using a key algorithm for authenticating communication between the KDC and the client such that all clients wishing access to the server are required to contact the KDC.

12. (Previously presented) The system of claim 4 further comprising requiring all entities wishing to access the server to communicate with the KDC.

13 - 17. (Cancelled)

18. (Previously presented) A system for detecting clones of a client within a communication network, the system comprising:

a KDC;

a server communicably coupled to the KDC;

a client for receiving an authentication token including an encrypted session key from the KDC, wherein the authentication token is for accessing the server, and is valid for a time duration T;

the server receiving from the client a first request to access the server, the first request being accompanied by the authentication token;

the server recording the time duration T for which the authentication token is valid;

the server receiving from an entity, a second request during the time duration T to access the server, the entity having identifying information identical to the client; and

the server either flagging or denying the second request to prevent access to the server.

19. (Cancelled)

20. (Original) The system of claim 18 further comprising necessitating by the system, all clients wishing to access the server to communicate with the KDC.

21. (Previously presented) The system of claim 18 wherein a ticket granting server is the server, and the ticket is a ticket granting ticket.

22. (Previously presented) A method for detecting clones in a communication network, the method comprising:

providing an authentication token including an encrypted session key to an authorized client, the authentication token for accessing a KDC, the session key valid for a time duration T;

receiving a request during time T to access the KDC, the request being received from an entity with the same identifying information as the authorized client; and

if the request is received during time T, flagging the entity as a possible clone or denying the request to access to the KDC.

23. (Cancelled)

24. (Original) The method of claim 1 wherein the KDC marks the entity as a possible clone or denies the second request in order to prevent access to the server.

25. (Original) The method of claim 1 wherein the server marks the entity as a possible clone or denies the second request in order to prevent access to the server.

26. (Previously presented) The system of claim 18 wherein the KDC is the server.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.